UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/937,819	10/29/2001	Volker Paul	5551	5425

6858 7590 06/10/2005

BREINER & BREINER, L.L.C.
P.O. BOX 19290
ALEXANDRIA, VA 22320-0290

EXAMINER	
ABRISHAMKAR, KAVEH	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 06/10/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/937,819	PAUL ET AL.	
	Examiner	Art Unit	
	Kaveh Abrishamkar	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 March 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-16* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-16* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This action is in response to the amendment received. on March 18, 2005. Claims 1-16 were originally received for consideration. Per the received amendment, claims 1-16 are amended. Claims 1-16 are currently being considered.

Response to Arguments

2. Applicant's arguments with respect to claims 1-16 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. Claims 1-11 are rejected under 35 U.S.C. 102(b) as being anticipated by Dorenbos (U.S. Patent No. 5,751,813).

Regarding claim 1, Dorenbos discloses:

A device for secure transmission respectively forwarding of coded data from a first data station via a second data station to a third data station of a network, comprising:

an input unit for receiving said coded data from said first data station and for receiving a requester's external key from said third data station or a further data station (column 2 lines 6-23, column 3 lines 5-57);

a unit for recoding said coded data by means of decoding with an internal key and renewed encoding with said external key, with said internal key not being accessible from outside said device (column 2 lines 6-23, column 3 lines 5-57); and

an output unit for issuing said data encoded with said external key (column 2 lines 6-23, column 3 lines 5-57);

wherein said device is designed in such a manner on or in said second data station that said unit for recoding recodes said data only upon request by said third data station with aid of said requester's external key and said data are not accessible in decoded form on said second data station from outside said device (column 2 lines 6-23, column 3 lines 5-57).

Claim 2 is rejected as applied above in rejecting claim 1. Furthermore, Dorenbos discloses:

The device according to claim 1, wherein said internal key is stored on a suited data carrier inside said unit (column 2 lines 6-23, column 3 lines 5-57), wherein the key

is stored on a server/computer which is well-known to have hardware to store encryption keys.

Claim 3 is rejected as applied above in rejecting claim 1. Furthermore, Dorenbos discloses:

The device according to claim 1 wherein said unit for recoding comprises a chip card as a carrier of said internal key (column 2 lines 6-23, column 3 lines 5-57), wherein the key is stored on a server/computer which is well-known to have hardware (chip card) to store encryption keys.

Claim 4 is rejected as applied above in rejecting claim 1. Furthermore, Dorenbos discloses:

The device according to claim 1, wherein said unit for recoding comprises an active chip card with an integrated processor, which partly or completely assumes decoding and encoding of said data (column 2 lines 6-23, column 3 lines 5-57).

Claim 5 is rejected as applied above in rejecting claims 1 to 4. Furthermore, Dorenbos discloses:

The device according to one of the claims 1 to 4, further comprising a buffer and logic unit for temporal control of data flow in said device, said buffer and logic unit first conveys said coded data for decoding to said unit for recoding and receives said data back decoded, and said buffer and logic unit subsequently conveys said decoded data

for encoding with said external key to said unit for recoding and receives said data back as coded data (column 2 lines 6-23, column 3 lines 5-57), wherein the data is first encrypted with a server public key and then decrypted in the server by a server private key (internal key) and then is encrypted with the receiver's public key (external key). Buffers are well-known in the art and are well-known in hardware.

Claim 6 is rejected as applied above in rejecting claim 1 to 4. Furthermore, Dorenbos discloses:

The device according to one of claims 1 to 4, wherein said input unit and said output unit are provided with standard interfaces for input and output of said data (column 2 lines 6-23, column 3 lines 5-57).

Claim 7 is rejected as applied above in rejecting claim 1 to 4. Furthermore, Dorenbos discloses:

The device according to one of the claims 1 to 4, wherein said unit for recoding utilizes asymmetrical encoding processes (column 2 lines 6-23, column 3 lines 5-57), wherein the system of Dorenbos uses public-private key encryption.

Claim 8 is rejected as applied above in rejecting claim 1 to 4. Furthermore, Dorenbos discloses:

The device according to one of the claims 1 to 4, further comprising a complete mechanical and electromagnetic encapsulation with a possibility of sealing (column 5 lines 53-60).

Claim 9 is rejected as applied above in rejecting claim 1 to 4. Furthermore, Dorenbos discloses:

The device according to one of claim to 4, further comprising a buffer unit which buffers all data flows inside said device to compensate for possible internal-key-dependent processing times so that data output of said device occurs according to a process-independent time span (column 2 lines 6-23, column 3 lines 5-57), wherein the data is first encrypted with a server public key and then decrypted in the server by a server private key (internal key) and then is encrypted with the receiver's public key (external key). Buffers are well-known in the art and are well-known in hardware.

Claim 10 is rejected as applied above in rejecting claim 1 to 4. Furthermore, Dorenbos discloses:

The device according to one of the claims 1 to 4, further comprising a unit for buffering current input of said device in such a manner that said current input of said device is independent of current input of said unit for recoding, which is dependent on said internal key, or of other internal circuits (column 2 lines 6-23, column 3 lines 5-57), wherein the data is first encrypted with a server public key and then decrypted in the server by a server private key (internal key) and then is encrypted with the receiver's

public key (external key). Buffers are well-known in the art and are well-known in hardware.

Claim 11 is rejected as applied above in rejecting claim 1 to 4. Furthermore, Dorenbos discloses:

The device according to one of claims 1 to 4, further comprising a unit for receiving a first data block containing said coded data in addition to further data and for separating said coded data from said further data and with a unit for joining said further data with recoded data to a second data block and for output of said second data block, with encoded data representing a key with which said further data are encoded (column 2 lines 6-23, column 3 lines 5-57).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 12-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dorenbos (U.S. Patent No. 5,751,813) in view of Kaufman et al. (U.S. Patent No. 5,764,772).

Regarding claim 12, Dorenbos discloses:

A process for secure data transmission of data from a first data station via a second data station to a third data station using the device according to claim 1, on or in said second data station, comprising:

encoding the data in first data station with a first key (column 2 lines 6-23, column 3 lines 5-57).

Dorenbos does not explicitly disclose that the first key is divided into a first part and a second part in such a manner that neither the first part or the second part alone can decode the coded data. Kaufman however disclose a system that a secret key (first key) is split into at least two partial keys such that knowledge of a first of the partial keys is not enough to break the encrypted message (Abstract). The systems of Dorenbos and Kaufman are analogous in that both transmit encrypted messages using asymmetrical encryption techniques (public/private key pairs). Furthermore, Kaufman encrypts the first partial key and is provided with the encrypted message. It would have been obvious that the receiver of the encrypted partial key and the encrypted message could be the encryption server as disclosed by Dorenbos, as it servers the same function as the authority, which decrypts the first partial key with a private key. Furthermore, as disclosed by Dorenbos, each recipient (a data station that wishes to receive the encrypted data) sends the public key that is used to recode the first partial key as it was used to recode the first key in Dorenbos (column 2 lines 6-23, column 3 lines 5-57). Both Dorenbos and Kaufman disclose decoding a first encrypted key (partial key in Kaufman) with a private key corresponding to the public key used to encrypt the first key (partial key). Furthermore, Dorenbos teaches after the decoding of

the first partial key, the recoding using the public key of the recipient so that the recipient may decode the partial key using the respective private key, when it is received. After the first partial key is decoded in the recipient (third data station), Kaufman discloses that the complete first key can be reconstructed by the recipient (Abstract). This complete secret key is then used in the system of Dorenbos-Kaufman to decrypt the encrypted message. It would have been obvious to one of ordinary skill in the art to use the partial keys of Kaufman in conjunction with the encryption server system of Dorenbos, so that if a partial key is compromised it "reduces but does not eliminate the work factor required to break the encrypted message" (Kaufman-Abstract). In the system of Dorenbos-Kaufman, the encrypted server becomes the middle step, instead of the endpoint as delineated in Kaufman. This combination is obvious because it provides a central server that can server multiple recipients by receiving their public key and recoding the key using their respective public keys.

Claim 13 is rejected as applied above in rejecting claim 12. Furthermore, Dorenbos discloses:

The process according to claim 12, wherein said first key is completely encoded and transmitted (column 2 lines 6-23, column 3 lines 5-57).

Claim 14 is rejected as applied above in rejecting claim. Dorenbos does not explicitly disclose only a part of the first key being encoded and transmitted to a second data station. Kaufman however disclose a system that a secret key (first key) is split into at

least two partial keys such that knowledge of a first of the partial keys is not enough to break the encrypted message (Abstract). The systems of Dorenbos and Kaufman are analogous in that both transmit encrypted messages using asymmetrical encryption techniques (public/private key pairs). Furthermore, Kaufman encrypts the first partial key and is provided with the encrypted message. It would have been obvious that the receiver of the encrypted partial key and the encrypted message could be the encryption server as disclosed by Dorenbos, as it servers the same function as the authority, which decrypts the first partial key with a private key. Furthermore, as disclosed by Dorenbos, each recipient (a data station that wishes to receive the encrypted data) sends the public key that is used to recode the first partial key as it was used to recode the first key in Dorenbos (column 2 lines 6-23, column 3 lines 5-57). It would have been obvious to one of ordinary skill in the art to use the partial keys of Kaufman in conjunction with the encryption server system of Dorenbos, so that if a partial key is compromised it "reduces but does not eliminate the work factor required to break the encrypted message" (Kaufman- Abstract).

Claim 15 is rejected as applied above in rejecting claims 12 to 14. Furthermore, Dorenbos discloses:

The process according to one of the claims 12 to 14 wherein said coded part of said first key is decoded in said third data station with said private key of said third station and subsequently said data are decoded with said first key (column 2 lines 6-23, column 5 lines 5-57).

Claim 16 is rejected as applied above in rejecting claims 12 to 14. Furthermore, Dorenbos discloses:

The process according to one of the claims 12 to 14, wherein said public key of said third data station is taken from an internal data bank of said second data station or is determined by consultation with a trust center (column 2 lines 6-23, column 5-57).

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kaveh Abrishamkar whose telephone number is 571-272-3786. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

KA
06/07/05

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER